Simplified LDAP Access Control Language System

ABSTRACT

A simplified LDAP access language system provides user-defined attributes that tell the directory system who the user wants to give read or write access to a specific set of his attributes. The read and write attributes are separate lists and may, in fact, differ, thereby giving the user the flexibility to better manage access to his attributes. The value of the read and write attributes are in an LDAP Filter format which is an Internet standard (RFC 2254) which allows the user to specify not only users local to his intranet, but users across the Internet as well. Access control lists (ACL) are created by the System Administrators and list the specific attributes that the user is allowed to control read or write access, giving the Administrators full control of what information the user can give out. The ACLs are stored in the directory along with the entries. When a user accesses an entry in a directory, the server checks the ACL specified for the attributes being accessed. The read or write attribute for the owner of the attributes being accessed are used by the server when it checks the ACL. The combination of the read or write attribute and the ACL determine whether the user has permission to perform the read or write access to the attribute being accessed.